

Popescu-Rohrlich correlations imply efficient instantaneous nonlocal quantum computation

Anne Broadbent*

Department of Mathematics and Statistics, University of Ottawa

In instantaneous nonlocal quantum computation, two parties cooperate in order to perform a quantum computation on their joint inputs, while being restricted to a *single* round of simultaneous communication. Previous results showed that instantaneous nonlocal quantum computation is possible, at the cost of an exponential amount of prior shared entanglement (in the size of the input). Here, we show that a *linear* amount of entanglement suffices, (in the size of the computation), as long as the parties share nonlocal correlations as given by the *Popescu-Rohrlich* box. This means that communication is not required for efficient instantaneous nonlocal quantum computation. Exploiting the well-known relation to position-based cryptography, our result also implies the impossibility of secure position-based cryptography against adversaries with non-signalling correlations. Furthermore, our construction establishes a quantum analogue of the classical communication complexity collapse under non-signalling correlations.

In two-party quantum computation, Alice and Bob wish to evaluate a quantum circuit C on their joint inputs. Here, we consider that Alice and Bob are *co-operating* players that are restricted only in the way they communicate: they can agree ahead of time on a joint strategy (and possibly establish shared correlations or entanglement), but they are separated before receiving their quantum inputs, and are allowed only a *single* round of simultaneous communication (thus: Alice sending a message to Bob, and Bob sending a message to Alice, *simultaneously*). The requirement is that at the end of this round, Alice and Bob must share the output system $\rho_{\text{out}}^{AB} = C(\rho_{\text{in}}^{AB})$. This problem is known as *instantaneous nonlocal quantum computation*. Remarkably, this task is known to be achievable for any circuit as long as the parties share an exponential (in the size of the inputs) amount of an entangled resource given as copies of the two-qubit maximally entangled state, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ [4, 13].

The motivation for the study of instantaneous nonlocal quantum computation includes the foundations of quantum physics and distributed computing; however, the original and main motivation is in the context of *position-based cryptography*. Here, parties use their geographic location as a cryptographic credential. Protocols typically exploit the relativistic no-signalling principle: the idea being that a careful timing argument would then ascertain the location of the parties[6]. Unfortunately, a no-go result is known in the the classical context[17]. Due to the quantum no-cloning principle, it was originally believed that quantum protocols could escape this impossibility result[16, 28–31]. However, these protocols are all broken by entanglement-based attacks, as long as the colluding adversaries share a large enough (exponential) amount of entanglement[4, 13]. This exponential overhead in resources (in terms of entanglement and quantum memory) leads to the main open problem in this area, which is to give a protocol which can be executed

efficiently by honest players, but for which any successful attack requires an exponential amount of resources (see related work[15, 40, 41]).

In an apparently unrelated line of research, Popescu and Rohrlich[38] defined the nonlocal box (*NLB*) as a virtual device that achieves the CHSH conditions[21] perfectly: when Alice (Bob) uses input x (y), the NLB produces output a (b) such that $a \oplus b = x \cdot y$. We note that quantum mechanics achieves this correlations with a maximum value of $\approx 85\%$ [20], but that the NLB is consistent with relativity since it does not enable communication. This device, as well as more general *non-signalling* correlations have been studied extensively, mostly in terms of understanding the power and limitations of *non-signalling* theories[3, 7, 11, 12], as well as more generally in terms of *information causality*[1, 14, 37] and *local orthogonality*[25, 39]; see also[32, 33]. One striking consequence of the NLB is that it implies the *collapse* of classical communication complexity[42], meaning that, any Boolean function can be computed in a two-party distributed context with a *single bit of communication*, as long as the parties have access to the NLB correlations[34]. This is presented as evidence against physical theories that allows the strong correlations of the NLB.

Here, we make progress towards the question of secure position-based quantum cryptography by showing an efficient attack to *any* scheme, where the participants are allowed the additional NLB resource. Our technique consists in showing that instantaneous nonlocal quantum computation is possible with a *linear* amount of pre-shared entanglement (in the size of the circuit), together with a linear amount of uses of the NLB. Furthermore, if we restrict the output to being a single qubit (say, held by Alice), the classical communication reduces to only two bits sent from Bob to Alice (in the case of quantum output), or a single bit (in the case of classical output). In both cases, this is optimal[5]. Thus our construction

establishes a quantum analogue of the classical communication complexity collapse[42] under no-signalling correlations.

Construction.—Our construction builds on the techniques of teleportation[5], gate teleportation[27], and quantum computing on encrypted data[8–10, 18, 23, 24] (see also [19, 43]). A key observation is that the Pauli-X and Z corrections used in teleportation correspond precisely to the process of quantum one-time pad encryption[2]. Thus, we view the two-party computation as being evaluated on encrypted quantum data, where the classical keys are available via the teleportation corrections. More precisely, for each wire i in the computation, Alice keeps track of encryption keys $x_i^A \in \{0, 1\}$ and $z_i^A \in \{0, 1\}$ (Bob does likewise with values $x_i^B \in \{0, 1\}$ and $z_i^B \in \{0, 1\}$). At any point in the computation, the keys are *distributed*: applying the operation $X^{x_i^A \oplus x_i^B} Z^{z_i^A \oplus z_i^B}$ at each wire i results in the quantum state at that point in the (unencrypted) computation. Crucially, the parties can evaluate the circuit on encrypted data *without any communication*: the decryption being delayed until the end of the protocol, when the parties exchange the classical keys and thus can locally decrypt (reconstruct) their outputs[35].

We represent the computation in the universal gate-set $X : |j\rangle \mapsto |j \oplus 1\rangle$ and $Z : |j\rangle \mapsto (-1)^j |j\rangle$, $H : |j\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + (-1)^j |1\rangle)$, $P : |j\rangle \mapsto i^j |j\rangle$. $CNOT : |j\rangle |k\rangle \mapsto |j\rangle |j \oplus k\rangle$, $T |j\rangle \mapsto e^{ij\pi/4} |j\rangle$, with all measurements being in the computational basis. At the onset of the computation, Bob uses shared entanglement to teleport his input registers to Alice; instead of sending the required Pauli corrections, he updates his local keys to represent these correction values. For the input wires originally held by Alice, Bob sets the keys to 0. Alice sets all of her keys to 0. Next, Alice locally performs the computation. All Clifford gates (X , Z , P , H , $CNOT$) are performed directly on the encrypted data, with both parties updating their keys after these gates, according to the well-known relationships between Pauli matrices and Clifford group operations[26] (see, e.g.[8, 18, 23, 24]).

The only remaining gate is the T -gate. Although this is a single-qubit gate, it is not in the Clifford group, and thus does not allow a simple re-interpretation of the encryption key; in fact: $TX^a Z^b = X^a Z^{a \oplus b} P^a T$ (up to global phase). Various methods have been proposed to evaluate the T on encrypted data[8, 10, 18, 23, 24]. We present in Fig. 1 a new method, that uses shared entanglement. The encryption of the output includes a distributed *multiplication*, $(x_i^A \oplus c) \cdot x_i^B$. Using the NLB correlations this can be re-linearized as $z^A \oplus z^B = (x_i^A \oplus c) \cdot x_i^B$. The local key updates are therefore $x_i'^A = x_i^A \oplus c$, $z_i'^A = z_i^A \oplus x_i^A \oplus z_i^A \oplus x_i^A \cdot c$, $x_i'^B = x_i^B$ and $z_i'^B = z_i^B \oplus x_i^B \oplus z_i^B \oplus d$. Correctness of Figure 1 can be seen by quantum circuit manipulations and identities, as presented further on. We note that our construction shows that the T -gate can be

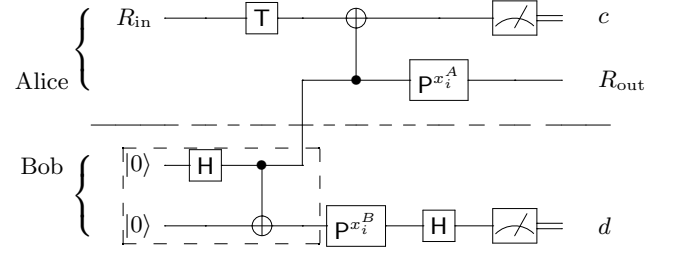


FIG. 1. Entanglement-based protocol for a T -gate on an input wire i held by Alice. The input wire $R_{in} = X^{x_i^A \oplus x_i^B} Z^{z_i^A \oplus z_i^B} |\psi\rangle$, and the output wire $R_{out} = X^{x_i^A \oplus x_i^B \oplus c} Z^{z_i^A \oplus x_i^B \oplus z_i^A \oplus x_i^A \cdot c \oplus (x_i^A \oplus c) \cdot x_i^B \oplus d} T |\psi\rangle$. The circuit in the dashed box prepares a two-qubit maximally entangled state and is executed before the computation begins.

computed in the two-party setting without any communication (but with the use of an NLB). This improves on prior work that required quantum[18, 23] or classical[9] communication.

It remains to show that the joint output of the computation can be obtained by a single round of simultaneous communication. This is accomplished by Alice using shared entanglement to teleport Bob's output registers to him; she then updates her Pauli keys accordingly. Next, both parties simultaneously exchange the classical keys required for decryption; a simple XOR calculation then allows each party to locally decrypt (reconstruct) their outputs [36].

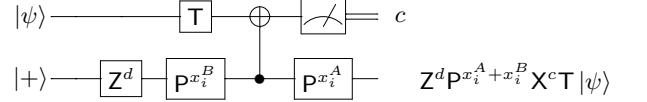


FIG. 2. Modified X -teleportation circuit

Correctness of the T -gate protocol.—In order to show correctness of Fig. 1, we consider a modification of the X -teleportation circuit[43] (Fig. 2), which can easily be seen as correct, since the diagonal gates Z and P commute with control. Furthermore, on input $X^{x_i^A \oplus x_i^B} Z^{z_i^A \oplus z_i^B} |\psi\rangle$, Fig. 2 produces the same output as in Fig. 1. Using the following identities (which hold up to global phase): $P^{a \oplus b} = Z^{a \cdot b} P^a$, $TX = PXT$, $TZ = ZT$, $XZ = ZX$, $PX = XZP$, $P^2 = Z$, we can compute the output as:

$$\begin{aligned} & Z^d P^{x_i^A + x_i^B} X^c T X^{x_i^A \oplus x_i^B} Z^{z_i^A \oplus z_i^B} |\psi\rangle \\ &= Z^{d \oplus x_i^A \cdot x_i^B} P^{x_i^A \oplus x_i^B} X^c P^{x_i^A \oplus x_i^B} X^{x_i^A \oplus x_i^B} Z^{z_i^A \oplus z_i^B} T |\psi\rangle \\ &= Z^{d \oplus x_i^A \cdot x_i^B} X^c Z^{c \cdot (x_i^A \oplus x_i^B)} Z^{x_i^A \oplus x_i^B} X^{x_i^A \oplus x_i^B} Z^{z_i^A \oplus z_i^B} T |\psi\rangle \\ &= X^{x_i^A \oplus x_i^B \oplus c} Z^{x_i^A \oplus x_i^B \oplus z_i^A \oplus x_i^A \cdot c \oplus (x_i^A \oplus c) \cdot x_i^B \oplus d} T |\psi\rangle \end{aligned}$$

Consequences.— The impossibility of position-based quantum cryptography using nonlocal correlations follows as a direct consequence of our construction. As for

the quantum analogue of the collapse of communication complexity, this follows by restricting the output to a single qubit (or bit) for Alice (and no output for Bob). In this case, Alice can reconstruct the output given only two classical bits from Bob (in the case that the output is classical, this is reduced to a single bit). This is optimal: in the quantum case, this follows from the optimality of teleportation[5], while in the classical case, any protocol with less than 1 bit of communication would violate relativity.

Since our result shows that communication is not required for efficient instantaneous nonlocal quantum computation, we have established a no-go result for position-based quantum cryptography against efficient adversaries with non-signalling correlations. This implies that, if position-based quantum cryptography is indeed possible against efficient quantum adversaries, it will be thanks in part to bounds such as Tsirelson's[20], according to which quantum mechanics is not maximally non-signalling. One open question that remains is to characterize more broadly the set of physical theories that rule out position-based cryptography, for instance, in terms of non-signalling correlations that are not known to be distillable to the NLB, or other related theories.

I would like to thank Gilles Brassard and Florian Speelman for fruitful discussions related to this work. This research is supported in part by Canada's NSERC.

* Part of this research was performed while the author was affiliated with IQC, University of Waterloo.

- [1] J. Allcock, N. Brunner, M. Pawłowski, and V. Scarani. Recovering part of the boundary between quantum and nonquantum correlations from information causality. *Phys. Rev. A*, 80:040103, 2009. DOI: 10.1103/PhysRevA.80.040103.
- [2] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *FOCS 2000*, pages 547–553, 2000. DOI: 10.1109/SFCS.2000.892142.
- [3] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71(2):022101, 2005. DOI: 10.1103/PhysRevA.71.022101.
- [4] S. Beigi and R. König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *N. J. Phys.*, 13(9), 2011. DOI: 10.1088/1367-2630/13/9/093036.
- [5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895, 1993. DOI: 10.1103/PhysRevLett.70.1895.
- [6] S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT 1993*, pages 344–359, 1993. DOI: 10.1007/3-540-48285-7_30.
- [7] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Phys. Rev. Lett.*, 96:250401, 2006. DOI: 10.1103/PhysRevLett.96.250401.
- [8] A. Broadbent. Delegating private quantum computations. *Can. J. Phys.*, 93(9):941–946, 2015. DOI: 10.1139/cjp-2015-0030.
- [9] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *FOCS 2009*, pages 517–526, 2009. DOI: 10.1109/FOCS.2009.36.
- [10] A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *CRYPTO 2015*, pages 609–629, 2015. DOI: 10.1007/978-3-662-48000-7_30.
- [11] A. Broadbent and A. A. Méthot. On the power of non-local boxes. *Theor. Comput. Sci.*, 358(1):3–14, 2006. DOI: 10.1016/j.tcs.2005.08.035.
- [12] N. Brunner and P. Skrzypczyk. Nonlocality distillation and postquantum theories with trivial communication complexity. *Phys. Rev. Lett.*, 102:160403, 2009. DOI: 10.1103/PhysRevLett.102.160403.
- [13] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-based quantum cryptography: Impossibility and Constructions. *SIAM J. Comp.*, 43(1):150–178, 2014. DOI: 10.1137/130913687.
- [14] D. Cavalcanti, A. Salles, and V. Scarani. Macroscopically local correlations can violate information causality. *Nat. Comm.*, 1:136, 2010. DOI: 10.1038/ncomms1138.
- [15] K. Chakraborty and A. Leverrier. Practical position-based quantum cryptography. *Phys. Rev. A*, 92:052304, 2015. DOI: 10.1103/PhysRevA.92.052304.
- [16] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky. Position-based quantum cryptography, 2010. [arXiv: 1005.1750](https://arxiv.org/abs/1005.1750).
- [17] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position based cryptography. In *CRYPTO 2009*, pages 391–407, 2009. DOI: 10.1007/978-3-642-03356-8_23.
- [18] A. M. Childs. Secure assisted quantum computation. *Quant. Inf. Comp.*, 5(6):456–466, 2005. Available online: <http://arxiv.org/abs/quant-ph/0111046>.
- [19] A. M. Childs, D. W. Leung, and M. A. Nielsen. Unified derivations of measurement-based schemes for quantum computation. *Phys. Rev. A*, 71(3):032318, 2005. DOI: 10.1103/PhysRevA.71.032318.
- [20] B. Cirel'son. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4(2):93–100, 1980. DOI: 10.1007/BF00417500.
- [21] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, 1969. DOI: 10.1103/PhysRevLett.23.880.
- [22] Y. Dulek, C. Schaffner, and F. Speelman. Quantum homomorphic encryption for polynomial-sized circuits, 2016. [arXiv: 1603.09717](https://arxiv.org/abs/1603.09717).
- [23] F. Dupuis, J. B. Nielsen, and L. Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In *CRYPTO 2010*, pages 685–706, 2010. DOI: 10.1007/978-3-642-14623-7_37.
- [24] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch. Quantum computing on encrypted data. *Nat. Comm.*, 5:3074, 2014. DOI: 10.1038/ncomms4074.
- [25] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín. Local orthogonality as a multipartite principle for quantum correlations.

- Nat. Comm.*, 4, 2013. DOI: 10.1038/ncomms3263.
- [26] D. Gottesman. The Heisenberg representation of quantum computers. In *GROUP 22*, pages 32–43, 1998. [arXiv: quant-ph/9807006](#).
 - [27] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. 402:390–393, 1999. DOI: 10.1038/46503.
 - [28] A. Kent, W. J. Munro, and T. P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84(1):012326, 2011. DOI: 10.1103/PhysRevA.84.012326.
 - [29] H.-K. Lau and H.-K. Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A*, 83(1):012322, 2011. DOI: 10.1103/PhysRevA.83.012322.
 - [30] R. A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81(4):042319, 2010. DOI: 10.1103/PhysRevA.81.042319.
 - [31] R. A. Malaney. Quantum location verification in noisy channels. In *Proceedings of the Global Communications Conference—GLOBECOM 2010*, pages 1–6. IEEE, 2010. DOI: 10.1109/GLOCOM.2010.5684009.
 - [32] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín. Almost quantum correlations. *Nat. Comm.*, 6, 2015. DOI: 10.1038/ncomms7288.
 - [33] M. Navascués and H. Wunderlich. A glance beyond the quantum model. *Proc. Roy. Soc. Lond. A*, 2009. DOI: 10.1098/rspa.2009.0453.
 - [34] This result was also shown by Richard Cleve (unpublished).
 - [35] Inspired by a 2011 preliminary report on this work, Speelman[40] used a similar framework to achieve instantaneous nonlocal quantum computation for circuits of low T -depth; recently, these techniques have led to the breakthrough result of *quantum fully homomorphic encryption*[22].
 - [36] We note that a variant of the protocol would forego the teleportation at both the beginning and the end of the protocol, instead using the *nonlocal* CNOT procedure from[23]. The resulting protocol has essentially the same properties, but may be beneficial in certain circumstances.
 - [37] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. Information causality as a physical principle. *Nat.*, 461(7267):1101–1104, 2009. DOI: 10.1038/nature08400.
 - [38] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Found. Phys.*, 24(3):379–385, 1994. DOI: 10.1007/BF02058098.
 - [39] A. B. Sainz, T. Fritz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín. Exploring the local orthogonality principle. *Phys. Rev. A*, 89:032117, 2014. DOI: 10.1103/PhysRevA.89.032117.
 - [40] F. Speelman. Instantaneous non-local computation of low T -depth quantum circuits, 2015. [arXiv: 1511.02839](#).
 - [41] D. Unruh. Quantum position verification in the random oracle model. In *EUROCRYPT 2014*, pages 1–18, 2014. DOI: 10.1007/978-3-662-44381-1_1.
 - [42] W. van Dam. Implausible consequences of super-strong nonlocality. *Nat. Comp.*, 12(1):9–12, 2013. DOI: 10.1007/s11047-012-9353-6.
 - [43] X. Zhou, D. W. Leung, and I. L. Chuang. Methodology for quantum logic gate construction. *Phys. Rev. A*, 62(5):052316, 2000. DOI: 10.1103/PhysRevA.62.052316.